I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Location-Sharing Technologies: Privacy Risks and Controls

JANICE Y. TSAI, PATRICK GAGE KELLEY,
LORRIE FAITH CRANOR, AND NORMAN SADEH*

Abstract: Due to the ability of cell phone providers to use cell phone towers to pinpoint users' locations, federal E911 requirements, the increasing popularity of GPS-capabilities in cellular phones, and the rise of cellular phones for Internet use, a plethora of new applications have been developed that share users' real-time location information online.[1] *This paper evaluates users' risk and benefit perceptions related to the use of these technologies and the privacy controls of existing location-sharing applications. We conducted an online survey of American Internet users (n = 587) to evaluate users' perceptions of the likelihood of several location-sharing use scenarios along with the magnitude of the benefit or harm of each scenario (e.g., being stalked or finding people in an emergency). We find that although the majority of our respondents had heard of location-sharing technologies (72.4%), they do not yet understand the potential value of these applications, and they have concerns about sharing their location information online. Most importantly, participants are extremely concerned about controlling who has access to their location. Generally, respondents feel the risks of using location-sharing technologies outweigh the benefits. Respondents felt that the most likely harms would stem from revealing the location of their home to others or being*

*Carnegie Mellon University Pittsburgh, PA jytsai@andrew.cmu.edu, pkelley@cs.cmu.edu, lorrie@cs.cmu.edu, sadeh@cs.cmu.edu.

[1] NORMAN SADEH, M-COMMERCE: TECHNOLOGIES, SERVICES, AND BUSINESS MODELS, Wiley (2002).

stalked. People felt the strongest benefits were being able to find people in an emergency and being able to track their children. We then analyzed existing commercial location-sharing applications' privacy controls (n = 89). We find that while location-sharing applications do not offer their users a diverse set of rules to control the disclosure of their location, they offer a modicum of privacy.

I. INTRODUCTION

By 2009, at least 87% of the U.S. population owned cellular phones.[2] The ubiquity of GPS-capabilities in mobile devices, federal E911 requirements, and the proliferation of mobile devices (including laptops) has spurred the development of location-sharing applications. These technologies, also referred to as mobile location technologies, social mobile applications, or simply location-based services ("LBS"), typically allow users to share their real-time or historical location information online. Despite the increased availability of these location-sharing applications, we have not yet seen wide adoption.[3] It has been suggested that the reason for this lack of usage may be users' privacy concerns regarding the sharing and use of their location information.[4] This paper seeks to explore the concerns regarding location-sharing technologies. In Section 1, we examine the use of LBS and research related to users' perceptions. Next, we investigate and enumerate the privacy controls offered by existing applications in Section 2. In Section 3, we present the results of an online survey to determine the magnitude of users' expected risks and benefits associated with these applications. Finally, in

---

[2] CTIA Wireless Association, Wireless Quick Facts: Year End Figures, http://www.ctia.org/media/industry_info/index.cfm/AID/10323 (last visited May 3, 2010).

[3] Corvida Raven, *What's plaguing your mobile social network?*, READWRITEWEB, May 15, 2008, http://www.readwriteweb.com/archives/whats_plaguing_your_mobile_soc.php (last visited May 3, 2010);

Caroline McCarthy, *The mobile social: Not ready for prime time?*, CNET NEWS BLOG, Feb. 13, 2008, http://www.news.com/8301-13577_3-9870611-36.html (last visited May 3, 2010).

[4] Louise Barkhuus et al., *From Awareness to Repartee: Sharing Location within Social Groups*, CHI 2008 PROC. 498-499 (2008); Laura M. Holson, *Privacy Lost: These Phones Can Find You*, N.Y. TIMES, Oct. 23, 2007, at A1; Iris A. Junglas & Richard T. Watson, *Location-Based Services*, COMM. OF THE ACM 51, No. 3 65-69 (2008); McCarthy, *supra* note 3.

Section 4 we evaluate the ability of existing location-sharing technologies to address user's perceived risks and provide recommendations for controls to address users' privacy concerns.

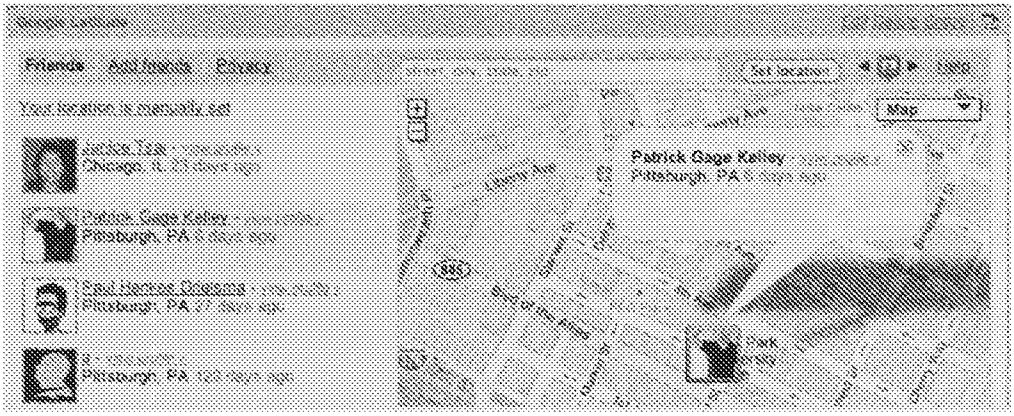

Figure 1: The web interface for Google Latitude

A. LOCATING TECHNOLOGIES

The location-information shared by LBS may be text-based (e.g. "Andrew has been located at 5000 Forbes Ave., Pittsburgh, PA"), or it may be map-based, where the user's location is represented as a dot on a map as illustrated in Figure 1 and Figure 2. To display location information, users can manually enter a street address or longitude and latitude coordinates. Today, location information is more frequently acquired through automated means. The following locating technologies are typically used to determine users' locations: GPS, wireless positioning, cellular identification, and IP identification.

The Global Positioning System ("GPS") locates a user through a device that is in communication with a constellation of satellites. Triangulation by multiple satellites locates the device, making GPS the most accurate method for finding locations.[5] However, drawbacks include the lack of user-accessible GPS capabilities in most personal cell phones and the scarce availability of built-in GPS technology in commercial laptops. Additionally, GPS can be battery intensive and inconsistent or unavailable indoors.

Wireless positioning is another common technology used. As urban areas become blanketed with both personal and public WiFi access points, users can be mapped according to their location relative

[5] SADEH, *supra* note 1, at 191.

to these access points. Through the process of "war-driving"[6] access points and mapping each broadcasting point to a GPS location,[7] researchers and companies such as Skyhook Wireless[8] have created large databases with high location accuracy. While these locations are not always as precise as GPS, more people have wireless devices and location information can be pinpointed indoors.

Cell phones or cellular identification can be used to locate users. At any given time, a mobile phone is likely in signal range of upwards of three cell phone towers, allowing a location to be triangulated if the locations of the cell towers are known. Some companies have partnered with telecom companies to use cellular data. One such company, AirSage, analyzes wireless signaling data to model traffic patterns. [9] Loopt, a location-sharing service, leverages a cellular partnership with AT&T to provide always-on location information based on a user's iPhone.[10]

---

[6] War driving is the act of locating wireless local area networks while driving around a city or elsewhere.

[7] Minkyong Kim et al., *Risks of Using AP Locations Discovered Through War Driving*, PERVASIVE 2006 67-82 (K.P. Fishkin et al. eds. 2006).

[8] Skyhook Wireless, http://www.skyhookwireless.com/ (last visited May 3, 2010).

[9] AirSage Real-Time Traffic , http://www.airsage.com/site/index.cfm?id_art=46770&vsprache=EN (last visited May 3, 2010).

[10] Dan Frommer, *Loopt Location to Update in the Background on iPhone*, BUSINESS INSIDER, Sept. 4, 2009, http://www.businessinsider.com/loopt-to-run-in-the-background-on-iphone-2009-6 (last visited May 3, 2010).

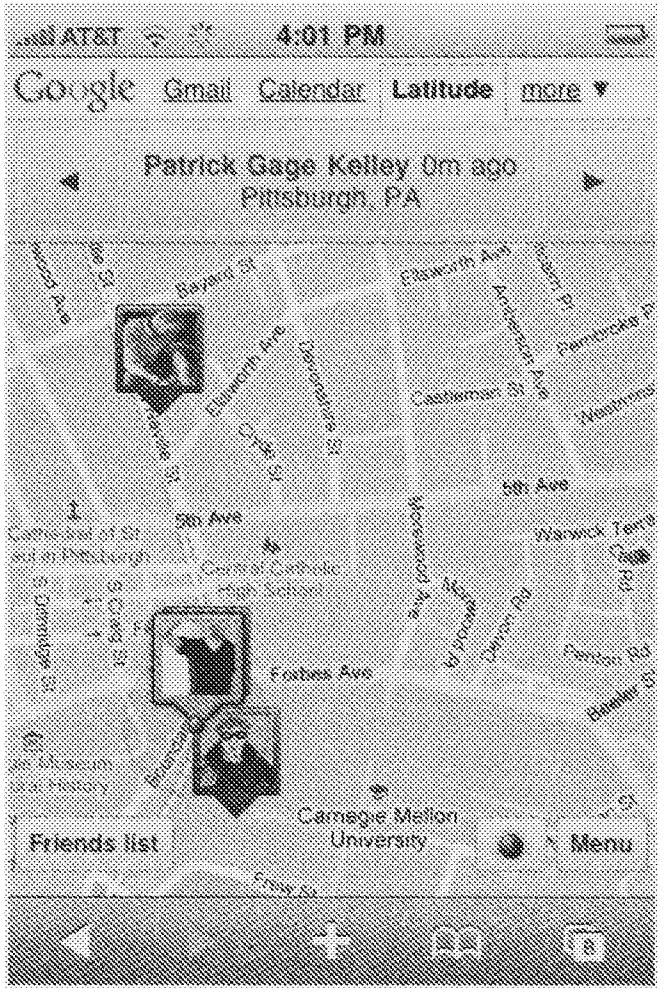

Figure 2: The iPhone interface for Google Latitude

Devices connected to an Internet network are provided with an IP address, which can be used to locate its user. IP addresses are limited in number and, and based on the range, can be associated geographically.[11] IP location is mostly used as a fallback when none of the above methods are available. The resolution of such lookups is commonly mapped to an area as large as a city.

[11] P.A. Roberts & S. Challinor, *IP Address Management*, BT TECHNOLOGY JOURNAL 18, No. 3 127-136 (2000). *See also* The IP-to-Country Database, http://ip-to-country.webhosting.info/ (last visited May 3, 2010).

B. DEVELOPMENT PLATFORMS FOR LOCATING-TECHNOLOGIES

Locating technologies are available for mobile phones, laptops, and internet-enabled mobile devices. There are three common ways for applications to pull location information: (1) through installed software, (2) a web browser, or (3) a location broker.

The first method to pull location information uses installed software. Users first download and install software onto their cell phones or computers. The software determines the user's approximate location by one of the methods listed above and stores that data in a database or sends it to a location-sharing application. This transmission of coordinates may be automatic (e.g., a location ping is sent every 5 minutes) or it may require a "push" action to be initiated by the user (e.g., the user clicks a "Find me now" button).

The second method makes use of a user's web browser. In lieu of requiring the user to run a separate piece of software, several companies have developed location-finding web browser plug-ins. Applications that use this technology locate users that visit a website, typically according to the users' wireless or IP location, based on an installed plug-in, such as Skyhook's[12] web toolbar Loki.[13]

The third is an application to get location information through a location broker. For example, APIs (e.g., Yahoo!'s FireEagle[14] and Google Latitude[15]) allow developers to create applications that pull the user's location from a central provider. This allows application developers to entirely avoid any of the location lookup technologies, relying on a third party to provide location information.

---

[12] Skyhook is a Wi-Fi positioning company that maintains a database of Wi-Fi access points and their geographic locations.

[13] Loki, http://loki.com/ (last visited May 3, 2010).

[14] FireEagle, http://fireeagle.yahoo.net/ (last visited May 3, 2010).

[15] Google Latitude, http://www.google.com/latitude/apps/badge (last visited May 3, 2010).

C. INDUSTRY BEST PRACTICES

The worldwide revenues from mobile marketing are projected to reach $24 billion in 2013.[16] It is understandable that the mobile or wireless industry would want to spur the adoption of location-sharing technologies. LBS may detect users' locations and offer them advertisements for businesses or services nearby. To address users' privacy concerns, CTIA, the International Association for the Wireless Telecommunications Industry, issued Best Practices and Guidelines for LBS providers.[17] These guidelines are meant to help LBS providers protect user privacy and rely on two of the Fair Information Principles ("FIPs"): user notice and consent.

Per the guidelines: first, LBS providers must inform users about how their location information will be used, disclosed, and protected so that a user can make an informed decision whether or not to use the LBS or authorize disclosure. Second, once a user has chosen to use an LBS or has authorized the disclosure of location information, he or she should have choices as to when or whether location information will be disclosed to third parties and should have the ability to revoke any such authorization.[18]

The CTIA guidelines do not specify the "form, placement, manner of delivery or content of notices."[19] Generally, providers post statements regarding notice and consent in their privacy policies or terms of service.

D. LOCATION PRIVACY STUDIES

Researchers have conducted studies to examine the usage of location-sharing applications and the privacy concerns they raise. These studies have employed the experience sampling method (ESM)

---

[16] *Mobile marketing revenue to hit $24 billion in 2013*, ABI RESEARCH, http://www.abiresearch.com/press/1037 (last visited May 3, 2010).

[17] CTIA WIRELESS ASSOCIATION, BEST PRACTICES AND GUIDELINES FOR LOCATION BASED SERVICES (2010), http://ctia.org/business_resources/wic/index.cfm/AID/11300 (last visited May 3, 2010)

[18] *Id.* at 1.

[19] *Id.* at 3.

where users have carried devices to simulate location requests.[20] Other experiments have involved small groups of participants who are members of existing social groups where people requesting locations were provided with automatic location disclosures,[21] or experimental designs where users respond via SMS with location information.[22] Field studies were conducted by the authors and their colleagues where a location-sharing application was deployed in a college campus community.[23]

Research has shown that the primary dimensions of privacy concern surrounding the disclosure of this information include context and use.[24] The willingness to share one's location and the level of detail shared depend highly on who is requesting the information[25] (or knowing that one's location is being requested[26]), and the social context of the request.[27] Due to users' varied privacy concerns and preferences depending on the situation[28] or activity in which the user

---

[20] Denise Anthony et al., *Privacy in Location-Aware Computing Environments*, in PERVASIVE COMPUTING 64, 64-72 (2007); Sunny Consolvo et al., *Location Disclosure to Social Relations: Why, When, & What People Want to Share*, CHI 2005 PROC. 81, 82 (2005); Ashraf Khalil & Kay Connelly, *Context-aware Telephony: Privacy Preferences and Sharing Patterns*, CSCW'06 (2006).

[21] Barkhuus et al., *supra* note 4; Barry Brown et al., *Locating Family Values: A Field Trial of the Whereabouts Clock*, in UBIQUITOUS COMPUTING 354, 354-371 (2007).

[22] G. Iachello et al., *Control, Deception, and Communication: Evaluating the Deployment of a Location-Enhanced Messaging Service*, in UBICOMP 213, 213-231 (2005); Ian Smith et al., *Social Disclosure of Place: From Location Technology to Communication Practices*, in PERVASIVE COMPUTING 134, 134-151 (2005).

[23] Janice Y. Tsai et al., *Who's Viewed You? The Impact of Feedback in a mobile location Sharing System*, CHI 2009 Proc. 2003, 2003-2012 (2009).

[24] Barkhuus et al., *supra* note 4; Louise Barkhuus & Anind Dey, *Location-Based Services for Mobile Telephony: a Study of Users' Privacy Concerns*, CHI 2008 PROC. 702, 702-712 (2003).

[25] Consolvo, *supra* note 20; Scott Lederer et al., *Who Wants to Know What When? Privacy Preference Determinants*, in UBIQUITOUS COMPUTING 724, 724-725 (2003).

[26] Tsai et al., *supra* note 23.

[27] Brown, *supra* note 21 at 354–71; Ashraf Khalil & Kay Connelly, "Context-aware Telephony: Privacy Preferences and Sharing Patterns" (paper presented at CSCW (2006).

[28] Lederer, *supra* note 25 at 724-5.

may be engaged,[29] privacy controls need to be flexible[30] and include a mechanism to provide plausible deniability.[31]

In addition to the context of a location request, it is users' own perceptions of the use of one's location information that impacts their privacy concerns.[32] For example, users may be more concerned with an acquaintance requesting their location because they are unsure of why that information is being requested compared to users' lack of concern when sharing location information with people nearby to find restaurant recommendations.

E. STUDIES OF PRIVACY CONTROLS

The lack of adequate controls for the disclosure of real-time personal information may be another cause of privacy concern. Studies that have examined rules discovered users desired diversity in the expressiveness of permissions in these types of systems.[33] In some cases, it may be enough for some users to simply create groups of contacts to assign permissions,[34] but others may require more flexibility in their rules.[35] In other research, it was found that a greater degree of rule expressiveness (e.g. being able to create group, time, and location-based rules) may increase the efficiency of allowing users to share information without violating their own personal privacy preferences.[36] Further relationship-based default rules and

---

[29] Iachello, *supra* note 22 at 213-32.

[30] Anthony, *supra* note 20 at 64-72; Norman Sadeh et. al., *Understanding and Capturing People's Privacy Policies in a Mobile Social Networking Application*, 13 Pers. Ubiquit. Comput. 401-412 (2009).

[31] Smith, *supra* note 22 at 134-51.

[32] Barkhuus & Dey, *supra* note 24 at 702-12; Consolvo *supra* note 20.

[33] Anthony, *supra* note 20 at 64-72; Michael Benisch et al., *The Impact of Expressiveness on the Effectiveness of Privacy Mechanisms for Location Sharing*, Tech. Rep. CMU-ISR-08-141, 2008, http://reports-archive.adm.cs.cmu.edu/anon/isr2008/CMU-ISR-08-141.pdf; Sameer Patil and Jennifer Lai, *Who Gets to Know What When: Configuring Privacy Permissions in an Awareness Application*,2005 CHI 101-10.

[34] Gary Hsieh et al., *Field Deployment of IMBuddy: A Study of Privacy Control and Feedback Mechanisms for Contextual IM*, 2007 UbiComp. 91-108; Patil & Lai, *supra* note 33 at 101-10.

[35] Anthony, *supra* note 20 at 64-72.

[36] Benisch, *supra* note 33.

machine learning techniques may reduce user burden in creating expressive rules.[37]

Based on this existing work, we delve into the design of commercial location-sharing systems and survey participants on their perceptions of the benefits and risks of specific scenarios of use for location-sharing systems.

II. AN EVALUATION OF PRIVACY CONTROLS IN LOCATION-SHARING APPLICATIONS

We examined 89 applications, social networks, and APIs to evaluate their privacy controls in April 2009. See the Appendix for a list of the applications. Our privacy and location-based services data is available online for download.

A. METHOD

We used a user-contributed online list of location-based services[38] as our directory of sites. In general, the sites on this list are social in nature. We found its completeness to be unparalleled across the web. We removed from consideration any sites that were not location-based services, or sites that were offline or defunct (n = 10). This left us with a final set of 89 applications.[39] We did not consider "surveillance technologies."[40]

To create our dataset, we completed a number of steps. We first visited the website for each application. We read the "About" page, frequently asked questions (FAQ), "Help" pages, and any other documentation available to search for explanations of their privacy controls. Additionally, we evaluated web interfaces, Facebook applications, and screen shots and descriptions of the iPhone application in the iTunes App Store. We evaluated the following features of these applications:

---

[37] Patrick Gage Kelley et al., *User-Controllable Learning of Security and Privacy Policies*, 2008 AISec 11–18.; Ramprasad Ravichandran et al., *Capturing Social Networking Privacy Preferences: Can Default Policies Help Alleviate Tradeoffs between Expressiveness and User Burden*, 2009 PETs 1-18.

[38] BDNOOZ, A list of Location Based Social Networking sites, http://bdnooz.com/lbsn-location-based-social-networking-links (last visited May 3, 2010).

[39] One of the applications included on the list, Locaccino, was developed by the authors.

[40] Surveillance technologies include items such as tracking devices used by detectives.

- **Date of launch:** While many of the current location-based services have relaunched, rebranded, or generally attempted to "reboot" their service, we have tried to find the most accurate date of a first public or widespread beta launch for each of the services. Many of these dates are based on news articles, press releases, and blogs that announced the opening of the service.

- **Privacy Policy:** We checked to see whether or not the website detailed their information practices (detailed in a privacy policy or included in a legal statement or terms of service).

- **Privacy Controls:** We noted any ability that allowed users to control access to their location information.

- **Notice:** Some systems notify users when others request their location, or make an activity log available to allow users to see who has requested and received their locations.

- **Immediately accessible privacy settings:** We noted whether or not the main interface allowed users to prominently see and access their privacy controls. For example, an application where one of the main tabs is labeled "Privacy" would fall under this category. An application that requires users to visit several pages or menus (e.g. Profile/Account/Settings/Privacy) does not.

B. DATA ANALYSIS

We constructed a dataset based on our collection of the features listed above. In this section, we present the results of our analysis.

1. SYSTEM CHARACTERISTICS

The primary purpose of the majority of these applications was for tracking friends or finding new ones. Other highlights included sites geared towards location-based dating, travel planning and sharing, and information seeking (e.g. finding local "hot spots"). One site even allows users to tag speed traps.

Of the 89 applications surveyed, 63 are available for use on mobile phones. Of those phone-based applications, the iPhone was the most popular development platform (40 applications). Application developers also created products for the Blackberry (32), phones that use the Android OS (21), or other phones (34). These numbers include services that developed a mobile formatted web version of their application and are not mutually exclusive. For example, a single service may have an iPhone application, a Blackberry application, and an Android application.

The architectures of the location-sharing applications fell into two categories: either open or closed. An open architecture allows users to be found by friends and strangers alike. The closed is more limited: users may only be requested by "friends" on the system. In this case, users must have already granted the requester access (e.g. by accepting a friend request).

Of the surveyed applications, five did not allow users to request other users' location information but allowed users to seek information about places or landmarks; and two are location-sharing APIs. Of the remaining sites, 29 are closed systems, and 52 are open systems.

2. RATE OF CREATION

The development of location-sharing applications has steadily increased over time as shown in Figure 3. Several new projects may have spurred the development of location-sharing technologies. These include the launch of Yahoo's FireEagle platform (Q1 2008) and the iPhone SDK[41] with its Core-Location framework (Q3 2008).

---

[41] Apple.com, iPhone Dev Center, http://developer.apple.com/iphone, (last visited May 3, 2010).

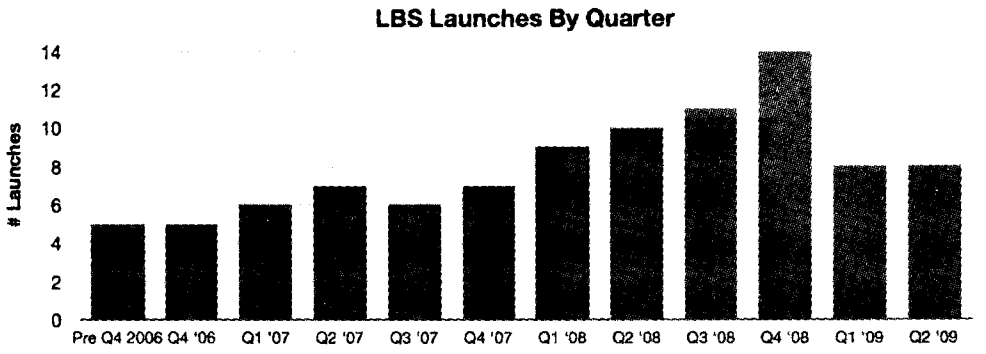

Figure 3: The number of location-sharing applications launched each quarter (includes 89 applications evaluated in our study and 7 defunct applications).

The rate at which location-based services were introduced to the market increased from five per quarter at the end of 2006 to fourteen per quarter at the end of 2008. After the economic downturn in 2008 the rate of introduction slowed, but new services continue to be introduced in 2009 at a rate of eight per quarter. This overall growth leads us to believe two things. First, development-side technologies are in place for location-based services and social networks to be created without unsolvable technical issues in the way of growth. Second, there do not seem to be strong market leaders who are prohibiting others from entering the market. Even with large players like Google and established brands like Loopt, we have not seen any one of these technologies spread to a large section of the populace (however, finding active user data for any of these services has proven to be difficult).

3. PRIVACY CONTROLS

Due to the sensitive nature of real-time location information and the existence of guidelines recommending clear notice to users, one would expect all location-sharing applications to detail their policies for the collection and use of personal information. Instead, we found that only 66% of the applications had privacy policies at all. For those services that did have privacy policies, the majority collect and save all data (e.g. locations, personal information entered into one's profile, and identifying web information such as one's IP address) for an indefinite amount of time. Only one, Mologogo, explicitly stated that

it deletes GPS data after one month.[42] Another interesting exception is Google Latitude, which stores only the most recent location update.[43]

Our review of location-sharing applications reveals that the majority have some form of privacy controls (76%). However, the majority of those privacy controls are not easily accessible from the main page or home page of the application itself. For the applications we reviewed, over 70% of them required users to visit or click multiple screens before we reached the privacy settings (see Table 1). This lack of immediately accessible privacy controls may be a result of the small amount of screen real estate available to application developers, especially in the case of mobile phones. For example, there was one case (Rummble[44]) included in the "Yes" category for accessible privacy settings in Table 1, where the web interface for the system had a link to the privacy controls, but the iPhone interface did not.

Category	Yes	No	Unknown	Not Applicable
Privacy Policy	66.3% (59)	33.7% (30)	-	
Privacy Controls	76.4% (68)	16.9% (15)	1.12% (1)	5.62% (5)
Accessible Privacy Settings	16.9% (15)	75.3% (67(	2.25% (2)	5.62% (5)

Table 1: An overview of the proportion of applications that have privacy policies, privacy controls, and explicit privacy settings.

The types of privacy controls for the location-sharing applications are the following:

- **Blacklist**: Users are able to block specific individuals from viewing their location. (Found in 15.7% (14) of services.)

- **Friends Only:** This whitelist-based control restricts access to users denoted as a "Friend."

---

[42] Mologogo.com, Mologogo Terms of Use, http://www.mologogo.com/terms.jsp (last viewed May 3, 2010).

[43] Google Latitude, Privacy, https://sites.google.com/a/pressatgoogle.com/latitude/privacy (last visited May 3, 2010).

[44] Rummble, http://www.rummble.com (last visited May 3, 2010).

By default, closed systems are considered friends only. (Found in 49.4% (44) of services.)

- **Granularity:** This advanced control allows users to instruct the system to provide a less detailed location to the person requesting information (e.g. "Andrew is in Pittsburgh, Pennsylvania.") (Found in 12.4% (11) of services.)

- **Group:** This restriction allows users to define access based on groupings of users. (e.g. Allow everyone in the "college friends" group to view my location.) (Found in 12.4% (11) of services.)

- **Invisible:** This feature may also be termed the "Private," "Only me," or "No one" setting. Users continue to send location data, but their locations are not divulged. (Found in 34.8% (31) of services.)

- **Location-based rules:** This restriction allows users to define locations in which their location-information may be revealed. For example, users may tag a location as "Work" or select an area on a map, and their location information is revealed to anyone who requests the user when they are at that location. (Found in 1.12% (1) of services.)

- **Network**: This restriction allows the user to select existing communities to whom their location may be revealed. For example, user may join a geographical network or an interest-based community with whom they wish to share their location. (Found in 12.4% (11) of services.)

- **Per-request permissions:** Users must specifically review each location request and decide whether or allow or deny the request prior to the location being revealed. (Found in 2.25% (2) of services.)

- **Time-based rules:** Users may define durations of time and days of the week during which their location may be revealed (e.g. from 10 am to 3 pm). (Found in 1.12% (1) of services.)

- **Time-expiring approval:** Several systems allow users to set a specific time frame (e.g. 1 hour) during which a link to the map of their location is "live." During this time frame, the recipient of the location message may view the map. After the expiration of this time, the link will no longer be accessible. (Found in 2.25% (2) of services.)

- **No restrictions:** Anyone is able to view the user's location. (Found in 16.9% (15) of services.)

- **Not Applicable:** Privacy controls do not apply. (Valid for 5.62% (5) of services.)

- **Unknown**: We were unable to find information about the privacy controls. (1.12% (1) of services.)

In general, we see that the "Friends Only" and "Invisible" restrictions are the most prevalent. Of the 89 applications we reviewed, only four provided explicit notice to the user regarding who had requested their location. Aka-Aki,[45] Locaccino,[46] and Mobiluck[47] provide request logs to the user so they can view "Who's Viewed Me," Sniff sends out a text message notification providing the name of the person making the request,[48] and HeyWay requires the user to

---

[45] Aka-Aki, http://www.aka-aki.com (last visited May 3, 2010).

[46] Locacinno, http://www.locaccino.org (last visited May 3, 2010) (the authors of this paper were also involved in the development of this application).

[47] Mobiluck, http://www.mobiluck.com (last visited May 3, 2010).

[48] Sniff, http://www.sniffu.com (last visited May 3, 2010).

explicitly approve or reject each location request (providing the name of the requester making the request).[49] The native Loki browser plug-in explicitly asks the user if an application making a request can access that information, but it does not provide the name of the person making the request. Only one specific application, Locaccino, had time-based and location-based rules.[50]

We reevaluated our list of 89 applications in February 2010. In the time from April 2009 to February 2010, 6 of the 89 applications no longer existed. Of the remainder, we found that there were no significant changes to the system characteristics nor the privacy controls offered by the applications.

III. LOCATION-SHARING RISK/BENEFIT ANALYSIS

We conducted an online survey to understand the magnitude of the risks and benefits associated with location-sharing services. We asked users to evaluate lists of risks and benefits and to rate the magnitude of benefit or harm associated with each item and the likelihood of each item occurring.

A. METHOD

For an individual user to adopt a technology, an acceptable balance of personal risk and benefits must be established.[51] To understand these risks and benefits, we investigated users' perceptions of location-sharing risks and benefits towards the use of location-sharing technologies. This evaluation takes into account the willingness or likelihood of engaging in the activity as a function of its expected benefit or harm.[52] We conducted an online survey to capture users' perceptions of how likely certain scenarios would be if they used location-sharing scenarios and the magnitude of benefits or risks related to each scenario.

---

[49] HeyWay, http://niftybrick.com/heyway.html (last visited May 3, 2010).

[50] Locaccino, http://www.locaccino.org (last visited May 3, 2010).

[51] Baruch Fischhoff, *Acceptable Risk: A Conceptual Proposal*, 1 RISK: HEALTH, SAFETY & ENVIRONMENT 1–28 (1994).

[52] Anne-Renee Blais and Elke U. Weber, *A Domain Specific Risk-Taking (DOSPERT) scale for adult populations*,1 JUDGMENT AND DECISION MAKING 34–37 (2006).

1. RECRUITMENT

In April 2008, we solicited participants to complete a survey to examine their personal perceptions about location-sharing technologies. Online announcements were posted on the "Volunteers" section of craigslist.com for major metropolitan areas of the United States and in online sweepstakes websites, recruiting individuals over the age of eighteen. The survey was available online for two weeks. We raffled a $75 Amazon.com gift certificate as the incentive for participation.

2. DEMOGRAPHICS

The final survey sample consisted of 587 respondents. Although 655 people completed the survey, respondents who completed the survey in under four minutes were eliminated from the final dataset. Due to the number of questions in the survey, we believed that anyone who answered in under four minutes was simply clicking through the survey rather than reading and responding to the questions. Participants' ages ranged from 18 to 79 years of age (M = 35.7), and 61% were female. The respondents were fairly well educated, with 43.8% indicating that they had college degrees and 29.1% having graduate degrees. In general, most people (72.4%) had heard of technologies that allow people to share their locations with others.

B. SURVEY DATA ANALYSIS

1. TECHNOLOGY USE

At the beginning of the survey, an example of an online-location sharing technology was presented to the study participants. A screen shot of a map with a thumbnail of a person's picture pinpointed on the map was displayed, indicating that the person had been located with this technology (see Figure 4). Participants were asked to list some benefits and risks or dangers associated with this technology. Some examples of benefits listed by our respondents are the following:

- Give out directions quickly to friends and family.

- Able to track loved ones and opportunity to surprise someone for a special event.

- People you know can find you, parents can track their kids, facilitates a rendezvous.
- Serendipitous encounters.
- Remote awareness of friends and relatives.

Some examples of dangers listed by our respondents are the following:

- Anyone could know exactly where you are - there is no privacy - anyone could find you at any given time.
- If someone intends to do you harm, they would find you easily.
- An unwanted person will find you and stalk you. It is not safe. You have no control.
- Location history could be harvested for stalking or marketing.
- People could find out if no one was home.

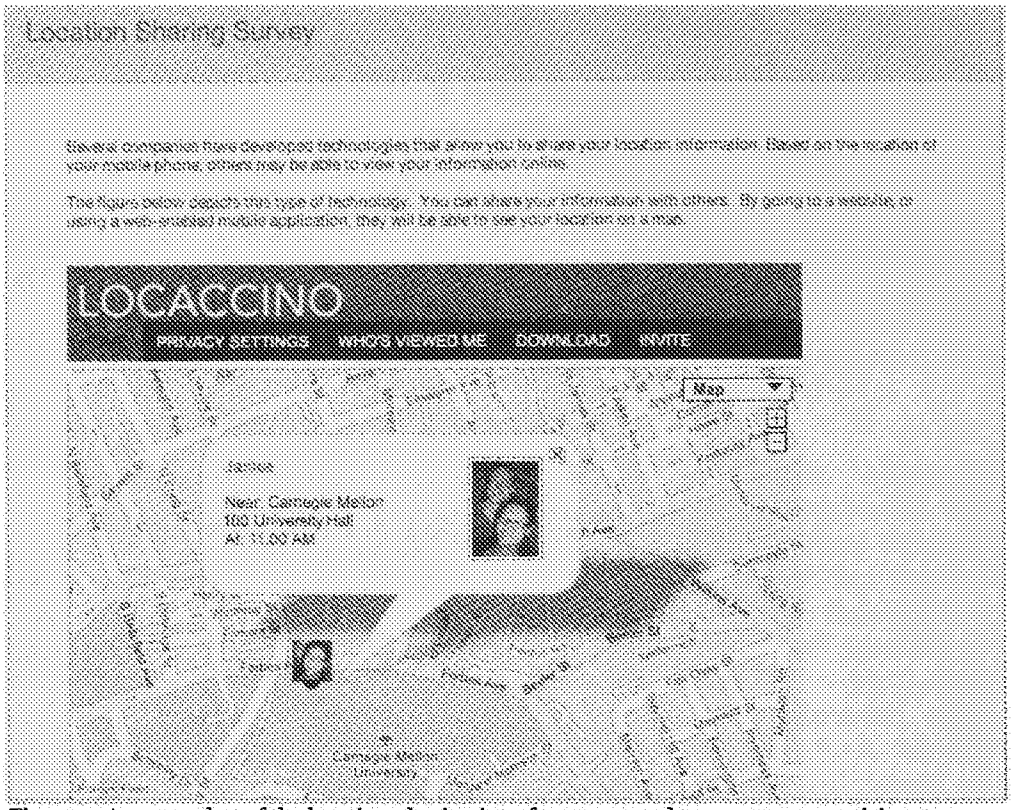

Figure 4: A screen shot of the location-sharing interface presented to our survey participants

Respondents were asked a series of 7-point Likert scale questions asking them to rate the usefulness of location-sharing technologies (ranging from *not useful* (1) to *extremely useful* (7)), their privacy concerns surrounding their use of these technologies (ranging from *not concerned* (1) to *extremely concerned* (7)), and the risk of using these applications (ranging from *the risk far outweighs the benefit* to the *benefit far outweighs the risk*). These questions were asked both at the beginning and end of the survey to determine if participating in the survey altered users' opinions.

The results reveal that people's first impression of location-sharing technologies is that they are mostly not useful. After taking the survey, which included various usage scenarios, people's opinions changed slightly, and they found the technology slightly more useful. They also became more concerned about allowing others to view their locations at the end of the survey. Participants' attitudes about the risk of using location-sharing technologies slightly outweighing the benefits did not change: they felt that the risk still outweighed the benefit. See Table 2 for mean values and paired t-test p values.

Item	Before	After	*t* statistic	*p* value
Usefulness	3.72	3.94	-3.91	<0.001
Concern	5.15	5.42	-4.66	<0.001
Risk	3.27	3.33	-1.01	0.31

Table 2: Participants' responses to 7-point Likert scale questions regarding the usefulness (not useful (1) to extremely useful) (7), concerns associated with allowing others to view your location (not concerned (1) to extremely concerned (7)), and the risk of using location-sharing technologies (the risk far outweighs the benefit (1) to the benefit far outweighs the risk (7)) at the beginning and end of the survey. The degrees of freedom for the paired t-tests is 586.

Item	M	t statistic	*p* value
You	3.84	-1.84	0.07
Family	3.67	-3.78	<0.001
Friends	4.3	4.05	<0.001
Company/Employer	3.63	-4.52	<0.001

Table 3: Participants' responses to 7-point Likert scale question regarding the likelihood of the use of location-sharing technologies (very unlikely (1) to very likely (7)). The responses are compared in a t-test to the midpoint (4). The degrees of freedom for the t-test are 567.

In the survey, we also asked participants about how concerned they were about controlling access to their location on a scale of *not concerned* (1) to *extremely concerned* (7). We found that participants were extremely concerned about having control (M = 6.17).

We also asked participants to rate the likelihood of the use of location-sharing technologies by them, their family, their friends, or their company or employer. Based on a 7-point Likert scale ranging from *very unlikely* (1) to *very likely* (7), we find that people think it is unlikely that their families and employers will use location-sharing technologies. As for themselves, they are neither likely nor unlikely to use the technologies, but think that their friends are more likely to use these types of applications. The responses to this question and their comparison to the midpoint of the scale are summarized in Table 3.

2. GENDER DIFFERENCES

Dividing participants by gender, we see that men find location-sharing technologies slightly more useful than women do, but men still find these technologies neither useful nor useless. Women are much more concerned with allowing others to view their locations, tend to feel that the risk of using these technologies far outweighs the benefit, and do not find it likely that they will use these technologies. These responses are detailed in Table 4.

Item	Female	Male	t statistic	*p* value
Usefulness	3.77	4.2	-2.78	0.006
Concern	5.6	5.14	3.73	<0.001
Risk	3.07	3.72	-4.19	<0.001
Likeliness of Use	3.56	4.26	-3.8	<0.001

Table 4: Participants' responses to 7-point Likert scale questions regarding the usefulness (not useful (1) to extremely useful) (7), concerns associated with allowing others to view your location (not concerned (1) to extremely concerned (7)), the risk of using location-sharing technologies (the risk far outweighs the benefit (1) to the benefit far outweighs the risk (7)) at the end of the survey, and the likeliness of use by the respondent. The degrees of freedom for the two-sample t-tests is 585.

3. SCENARIOS

We asked participants to rate the likelihood of the occurrence of the scenarios below on a 7-point Likert scale from *very unlikely* to *very likely*. Each scenario is also rated as a harm or a benefit. For each of the harms scenarios, participants were asked to rate each harm from a scale from *not harmful at all* (1) to *extremely harmful* (7). For each of the benefits scenarios, participants were asked to rate each benefit on a scale from *no benefits at all* (1) to *great benefit* (7).

The responses to the scenarios are detailed in Table 5 and Table 6

Scenario	Likelihood	Benefit
Finding people in an emergency	5.64	5.97
Finding information based on your location	5.29	4.99
Keeping track of the location of children in your family	5.17	5.18
Checking people's locations to make sure they are ok	4.98	5.05

Finding nearby friends for social activities	4.76	4.36
Using people's locations to coordinate a meeting	4.67	4.34
Keeping track of elderly relatives	4.66	5.11
Keeping track of where you've been	4.65	3.84
Coordinating family activities	4.59	4.39
Finding a coworker who is running late for a meeting	4.42	4.03
Coordinating ride sharing or carpooling	4.38	4.29
Having fun with locations	4.35	3.47
Recruiting people to participate in activities	4.01	3.83
Finding new people with similar interests	3.49	3.46

Table 5: Benefits-based location-sharing scenarios and their likelihood and magnitude of benefit ratings based on survey results, ordered by highest likelihood.

There were several scenarios in which people would be extremely likely to benefit from such services: finding people in an emergency, finding information based on location, and finding (tracking) their children. Based on the survey results, people also seem to realize that using location- sharing technologies will likely open them to receiving advertisements based on their location, being intruded upon, as well as accidentally revealing the location of their homes.

Scenario	Likelihood	Harms
Being bothered by ads that use your location	5.27	4.68
Having people intrude on your private space	5.15	5.51
Revealing the location of your home	5.11	5.93
Being found by someone you don't want to see	5.1	5.56
Being found when you want to be alone	5.07	5.08
Revealing activities you are participating in	4.83	4.17
Being stalked	4.75	6.32
Having the government track you	4.72	5.38
Being judged based on your location	4.35	4.5
Having your boss spy on you	4.21	5.15

Table 6: Risk-based location-sharing scenarios and their likelihood and magnitude of harm ratings based on survey results, ordered by highest likelihood.

4. LEVEL OF PRIVACY CONCERN

We sought to determine the level of privacy concerns that people perceive when they are sharing their information online by asking several privacy scale questions. These privacy scale questions are based on an instrument developed by Malhotra et al. to measure Internet Users' Information Privacy Concerns (IUIPC).[53] The IUIPC scale defines several groupings of concern, including control, awareness of privacy practices, collection of information, errors, unauthorized secondary use, improper access, and global information privacy concern; and consists of 27 questions. Based on a pilot test where we correlated the use of Facebook, an online social network, and the use of its privacy settings, we selected a sampling of six questions. Based on these questions, we calculated a "privacy score" for each respondent. This score is an average of the ratings of the following six statements presented to the users, rated on a 7-point Likert scale, ranging from *strongly disagree* (1) to *strongly agree* (7). The higher the privacy score, the more concerned the person is about their privacy.

- Participants were asked to rate the following statements:
- It is very important to me that I am aware and knowledgeable about how my personal information will be used. (IUIPC Awareness)
- I'm concerned that online companies are collecting too much personal information about me. (IUIPC Collection)
- Online companies should have better procedures to correct errors in personal information. (IUIPC Errors)
- Online companies should never share personal information with other companies unless it has been authorized by the individuals who

---

53 Naresh K. Malhorta, Sung S. Kim, and James Agarwal, *Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model*, 15 INFORMATION SYSTEMS 336, 351-352 (2004).

provided the information. (IUIPC Unauthorized secondary use)

- Online companies should take more steps to make sure that unauthorized people cannot access personal information in their databases/servers. (IUIPC Access)

- I am concerned about threats to my personal privacy today. (IUIPC Global Concern)

To determine if this scale was internally reliable, we computed a Cronbach's α score for this set of questions. This statistic allows us to determine if the items, together, measure a consistent viewpoint. A set of items with a Cronbach's α score of above 0.70 is considered to be reliable. We found this 6-item scale for assessing users' privacy concerns regarding online companies to be reliable, with a Chronbach's α of 0.85.

To determine if the privacy score had any relation to users' use and perceptions of location- sharing technologies, we examined their correlations. We see that the higher the privacy score, the more likely it is that users will feel that the risks of using location-sharing technologies outweigh the benefits (Risk After, $r(586) = -0.23$, $p < .0001$), that they would be less likely to use such technologies ($r(586) = -0.12$, $p = 0.004$), and that they feel that this technology is not useful (Usefulness After, $r(586) = -0.11$, $p = .007$). Additionally, users with higher privacy scores were older ($r(586) = 0.23$, $p < .0001$), more concerned about privacy (Concern After, $r(586) = 0.41$, $p < .0001$), and more concerned about controlling access to their location($r(586) = 0.39$, $p < .0001$).

5. Expected Values of Risks and Benefits

To examine the ranking of the scenarios, we computed an expected value for the risk variable by multiplying the likelihood perceptions by the magnitude of the risk (harms) or benefit. This value allows us to compare within the sets of scenarios that are considered harms and those that are considered benefits. We can also see the priority of those harms and benefits.

Within each set of harms and benefits, the expected value for the risk (or benefit) of each was compared to the other harms or benefits with paired t-tests to determine which scenarios are significantly distinct from each other ($p < 0.05$). The relative rankings for the

benefits and risks as determined by their expected value are summarized in 7 and Table 8.

Ranking	Scenario
1	Finding people in an emergency
2	Keeping track of the location of children in your family
3	Finding information based on your location
3	Checking people's locations to make sure they are ok
3	Keeping track of elderly relatives
4	Finding nearby friends for social activities
4	Using people's locations to coordinate a meeting
4	Coordinating family activities
5	Coordinating ride sharing or carpooling
5	Discovering that a friend from out of town is visiting
6	Keeping track of where you've been
6	Finding a coworker who is running late for a meeting
7	Recruiting people to participate in activities
7	Having fun with locations (e.g. games, pranks)
8	Finding new people with similar interests

Table 7: The relative rankings of benefits obtained from the use of location-sharing technologies.

Ranking	Scenario
1	Revealing the location of your home to people you do not want to give your address to
1	Being stalked
2	Having people intrude on your private space
2	Being found by someone you don't want to see
3	Being found when you want to be alone
3	Having the government track you
3	Being bothered by ads that use your location
4	Having your boss spy on you
5	Revealing activities you are participating in
5	Being judged based on your location

Table 8: The relative rankings of risks related to the use of location-sharing technologies.

Evaluating each expected benefit, one sees that, by far, the most significant benefit is being able to find people in an emergency. The next distinct benefit is being able to track one's children. Finding information based on one's location, checking to see if people are ok, and tracking relatives are the third set of distinct benefits. The least

valued expected benefit of location-sharing technologies is finding new people based on one's location.

The greatest expected harms derived from the use of location-based technologies are revealing one's home and being stalked. People perceive that being found by people one wants to avoid and having others intrude on one's personal space are the next set of situations associated with these technologies. Being found when one wants to be alone, being tracked by the government, and receiving ads based on one's locations are the third set of distinct harms. It seems that people are the least bothered by the risks of being judged based on one's location and revealing activities in which one is participating.

6. Analysis of Participants with Children

One potentially useful scenario for location-sharing technologies is keeping track of children in one's family. We asked participants to list the number of children they had and divided our participants into two categories: those who have children and those who do not. The group with children includes those with adult children. Demographics are summarized in Table 9. We see that having children does have an impact on one's perceptions of these technologies.

Item	Without Children	With Children
Gender	Fem: 218; Male 147	Fem: 140; Male: 82
Avg. Age	30.9	43.7

Table 9: Participants characterized by whether or not they have children or do not have children.

Participants with children rated location-sharing technologies significantly more useful at the beginning of the survey as compared to participants without children (MWithChildren = 3.93 vs. MWithoutChildren = 3.59, $t(585) = -2.17$, $p = 0.03$). After taking the survey, both groups felt the same about location-sharing technologies being neither useful nor not useful (MWithChildren = 4.08 vs. MWithoutChildren = 3.85, $t(585) = -1.5$, $p = 0.13$).

When asked about the likelihood of use of these types of technologies, participants with children were significantly more likely to feel that they, their families, friends and employers would be likely to use these technologies as compared to people without children. See Table 10 for details of survey results and t-tests.

Item	Without Children	With Children	t statistic	*p* value
You	3.67	4.11	24.01	**<0.001**
Family	3.32	4.26	28.36	**<0.001**
Friends	4.27	4.36	26.52	**<0.001**
Company/Employer	3.48	3.87	26.21	**<0.001**

Table 10: Participants' responses to 7-point Likert scale question regarding the likelihood of the use of location-sharing technologies (very unlikely (1) to very likely (7)) for people without children and with children. The degrees of freedom for the t-test are 585.

Examining the responses to the scenarios, we see that participants with children derived greater expected benefit, as compared to respondents without children from the following scenarios: checking people's locations to make sure they are okay, coordinating family activities, keeping track of the location of children in your family, keeping track of elderly relatives, and finding new people with similar interests. Those with children also had a greater amount of expected risk from being bothered by ads that use their location, being tracked by the government, and revealing activities they are participating in. These differences are detailed in Table 11.

Item	Without Children	With Children	t statistic	*p* value
Okayness Checking	25	29.9	-4.06	**<0.001**
Coordinating Family Activities	20.5	26.1	-4.65	**<0.001**
Tracking Children	26.1	34.6	-6.18	**<0.001**
Tracking Relatives	24.2	29.9	-4.12	**<0.001**
Finding New People	13	16	-2.8	**0.005**
Bothered by Ads	24.7	27.7	-2.35	**0.02**
Tracked by the Government	25.3	28	-1.98	**0.05**
Revealing One's Activities	20.1	22.4	-2.08	**0.04**

Table 11: Participants' expected benefits and risks based on if they have children or if they do not have children. The values were calculated by multiplying the likelihood ratings of each scenario with its rated risk and benefit. Degrees of freedom for the two-sample t-tests are 585.

For respondents with children, being able to track their kids becomes the top benefit, tied with being able to find people in an emergency. Even when we control for age and gender, we find this to be the case.

IV. THE ABILITY OF LBS APPLICATIONS TO ADDRESS USERS' PERCEIVED RISKS

As location-based services proliferate in numbers but not in users,[54] we examined the ability for these location-sharing applications to address users' privacy concerns. We see that the number of applications has been increasing and companies have developed platforms that make it easier for others to create applications that leverage location information. Based on the results of our survey, we see that people still do not find these location-sharing technologies all that useful, and they are still concerned about their privacy when sharing their locations online. In general, people still believe that the risks of sharing their locations online outweigh the benefits.

Based on our analysis of the risks associated with these technologies, we now examine the existing privacy controls of these technologies and investigate the ways in which these controls can address users' major concerns. We also suggest additional methods of addressing users' concerns.

A. ADDRESSING RISKS WITH PRIVACY CONTROLS

To determine if privacy controls are effective in location-sharing technologies, we first examine users' greatest expected risks.

As enumerated in Table 8, we see that the top ranked expected risks are the following: revealing the location of your home to people you do not want to give your address to; being stalked; having people intrude on your private space; being found by someone you don't want to see; being found when you want to be alone; having the government track you; and being bothered by ads that use your location. Below, we examine how location-based applications' privacy controls address these concerns:

Blacklist: With blacklists, users are able to block specific people with whom they do not wish to reveal their location. This restriction allows users to protect against revealing the location of their homes and block known stalkers and people they do not wish to see. If users are active in managing and updating their blacklists, they may also reduce the ability of people to intrude on their space and avoid being

---

54 Corvida, *What's Plaguing Your Mobile Social Network?*, READWRITEWEB, May 15, 2008, http://www.readwriteweb.com/archives/whats_plaguing_your_mobile_soc.php; Caroline McCarthy, *The Mobile Social: Not Ready for Prime Time?*, NEWS.COM, Feb. 13, 2008, http://www.news.com/8301-13577_3-9870611-36.html.

found when they want to be alone. Unfortunately, in the last two cases, users must spend the effort and time to add people to a blacklist and must remember to remove people from the blacklist once they want to be found again.

Friends Only: By only allowing friends to access users' locations, users are protected from being stalked (users may remove their stalkers from their friend lists). Unfortunately, this control does not protect one from being found by friends when one wants to be alone or being found by someone who is a friend, but whom the user may not wish to see. To deal with these concerns, users may manage their friend lists by adding and removing friends as they see fit.

Granularity: Allowing the location-sharing application to only provide general information (e.g. neighborhood, city, or state) about one's location mitigates the risks (except for being bothered by ads and being tracked by the government). Unfortunately, by only providing a wide range of possible locations, this also negates the benefits provided by location-sharing applications.

Group-based rules: Allowing people access to your location by dividing them into groups mitigates several privacy concerns. These group-based rules allow users to protect the location of their homes, to hide themselves from stalkers, and to avoid people they do not want to see. Based on how large the group is and how active they are in assigning people to groups may also reduce, but not eliminate, the risks of having people intrude on their private space and being found when they want to be alone.

Invisible: By going invisible, the user reduces the risks listed above except for that of being bothered by location-based ads and government tracking. Users can significantly reduce the risk of being stalked or of being found by people they don't want to see, but they also reduce the benefits of these services. To most effectively deal with the risks, they must be very active in turning invisible mode on and off, which places a significant burden on the user.

Location-based rules: Defining access by location allows the user to effectively protect the location of his home or spaces in which one needs private space or alone time. These rules may also block known stalkers at locations they do not wish to reveal. By continuously updating these rules, users may effectively address most of the risks, but this requires users to regularly update their rules.

Network: A network is typically larger than a group (e.g. the Chicago network). This may make it easier for users to define rules, but may not be an effective means in protecting them from the risks listed above. By defining network based rules, one prevents the general public from locating them, but may not keep stalkers within their network from finding them, or it may not prevent others from

finding the location of their home, or preserving their personal space and alone time.

Per request permission: Requiring users to approve each location request reduces the risks listed above except for that of being tracked by the government and being bothered by ads. Unfortunately, this method requires that users be interrupted, and this may become too burdensome on the user.

Time-based rules: Basing restrictions on time allows users to create restrictions to protect the locations of their homes (assuming they are home at regular times). Time-based restrictions can also protect users from being intruded upon, being found, and allows them to be alone at certain times of the day or days of the week.

Time-expiring approval: Allowing users to specifically permit others to locate them mitigates most risks (excluding government tracking and being served with advertisements based on their location). Unfortunately, allowing users to be the only ones to "push" location information also negates most of the top benefits of location sharing (e.g. one would not be able to find someone in the case of an emergency when they need to wait for the user to make his location available for a small period of time).

No restrictions: Having no rules allows users to be located by anyone. This opens them up to all the benefits as well as the risks of using location-sharing technologies.

We see that the rules that allow users to mitigate the greatest risks are the following:

- Blacklist
- Granularity
- Group-based rules
- Location-based rules
- Time-based rules

Each of these rules alone, including the burden on the user, does not address the largest expected risks of using location-sharing technologies. We find that location-sharing technologies offer limited flexibility in their privacy controls. It is rare that systems give users the ability to specify expressive rules to control the sharing of their location information. Furthermore, there are no commercially available systems that offer anywhere near as powerful a control set as

one could imagine: with the ability to specify rules based on specific users and groups of contacts, to control access based on time and location, to return locations at varying granularities, and to become invisible or obfuscate locations in extreme situations. There is one system, Locaccino, developed by the authors' university, that offers time, location, and group based rules, as well as invisibility.[55] A combination of all of these rules would be the most effective in addressing users' privacy concerns.

Another factor that has been mentioned briefly is user burden. In some cases, it would be possible for the user to toggle being invisible on and off all day based on that day's events. Unfortunately, in our experience, people easily forget to do this. Once the location-sharing software is up and running, it is easier to leave it running; otherwise, once people go offline or invisible, they are likely to leave the software in that setting. Similarly, in systems that do offer a myriad of privacy controls, methods must be developed to help users create rules based on their daily schedules along with their regular and irregular interactions with others.

B. DISCUSSION

By defining the relative value of users' expected risks and benefits regarding the use of location-sharing services, we develop an understanding of users' privacy concerns. We see that, in general, industry guidelines do not address these concerns, and the privacy controls in existing applications do not comprehensively address these concerns. In this paper, we have provided recommendations for sets of privacy control that may assist developers in addressing users' privacy concerns.

Based on the current perceptions of benefits and harms of location-sharing technologies at this time (noting that perceptions of risks in this area may evolve or shift), the primary risks can be addressed or mitigated by the design of the location-sharing technology. Based on the current restrictions offered by location-sharing technologies, we find that these risks may not be addressed, in full, by the current palette of available privacy controls. Instead, location-sharing applications may want to consider making more expressive privacy controls available to their users. With more expressive controls, people may become more comfortable with sharing their location information and find more value in these

---

[55] Sadeh, *supra* note 30.

services. Additionally, future work must be done to determine how to reduce user burden. A balance must be found between expressiveness and usability, or between offering users complex and detailed privacy controls and making these controls easy to use.

Another matter to consider is that of users' evolving privacy concerns. Currently, we find that users' still do not find location-sharing services useful. This may be because of the lack of usage in general. Without a critical mass of users, current users are unable to reap the benefits of being able to find their friends or to track family members. As more and more people adopt these types of technologies, and peer opinion about these technologies becomes more favorable, the level of concern that people feel may diminish. Additionally, we find that younger people or people with children are more interested in location-sharing applications and are more likely to adopt these services.

V. ACKOWLEDGEMENTS

This work is supported in part by the National Science Foundation through Cyber Trust grant CNS-0627513, CNS-0905562, and DGE-0903659; and by the Army Research Office contract no. DAAD19-02-1-0389 to Carnegie Mellon University's CyLab. Additional support has been provided by Microsoft through the Carnegie Mellon Center for Computational Thinking, and FCT through the CMU/Portugal Information and Communication Technologies Institute.